JUN 14 2004
PATENT & TRADEMARK OFFICE

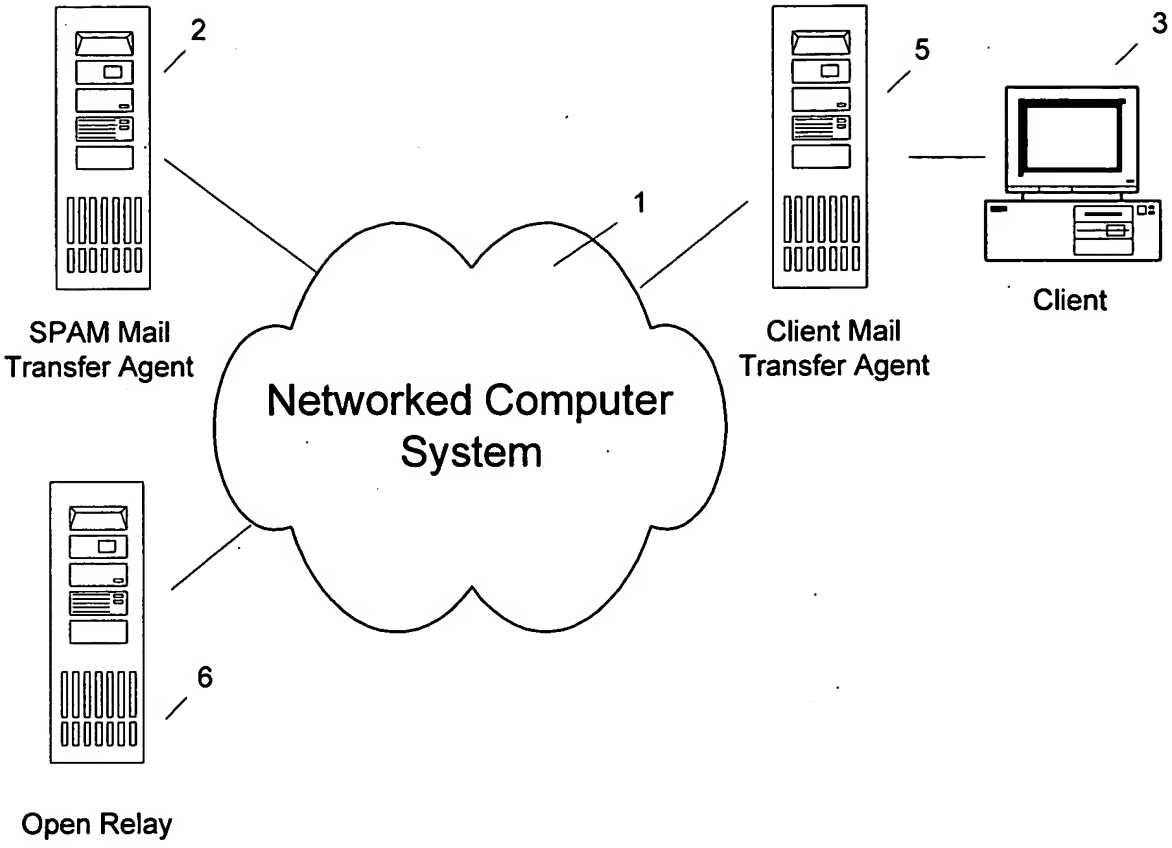

Fig. 1 (prior art)

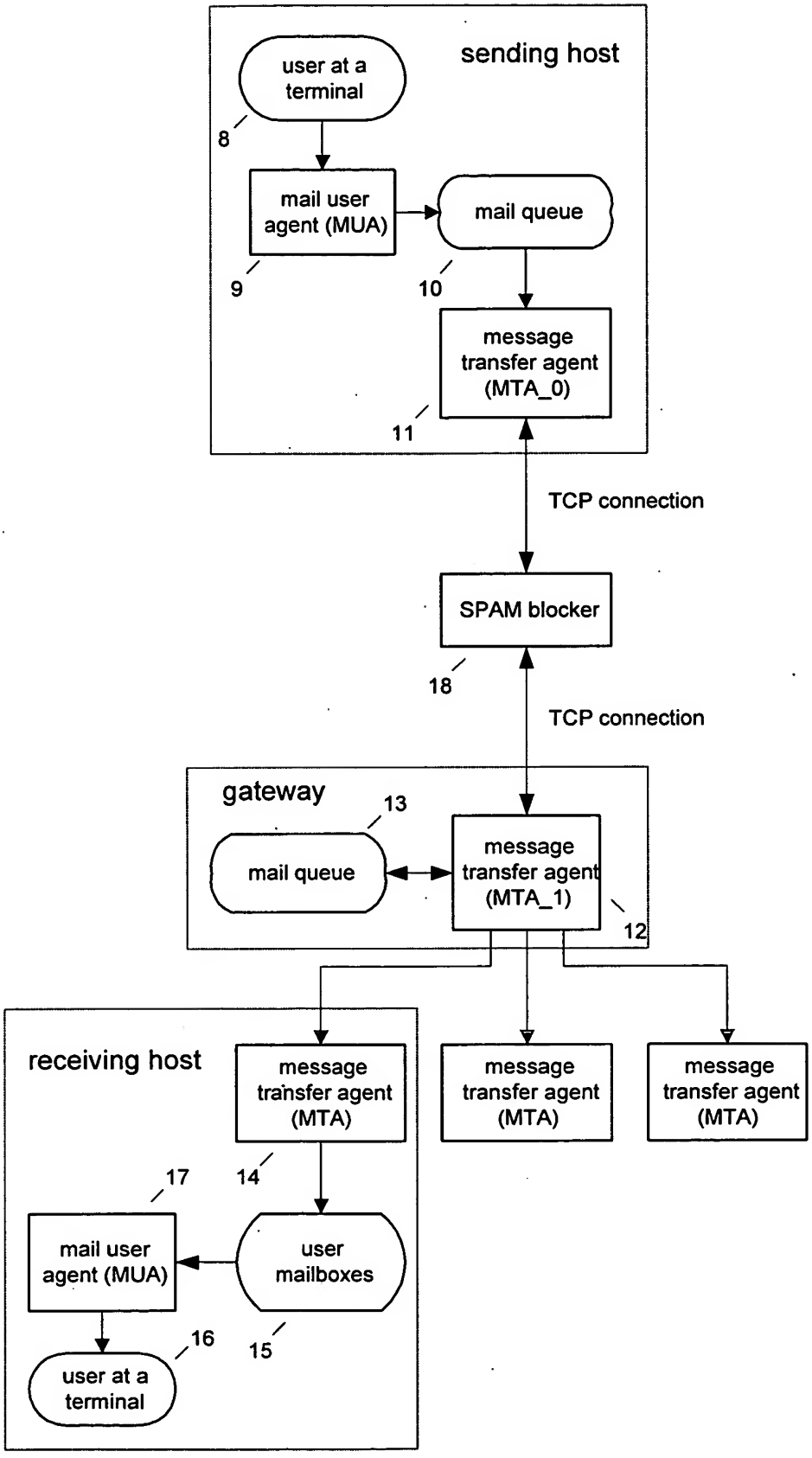
sending host
user at a terminal
8
mail user agent (MUA)
9
mail queue
10
message transfer agent (MTA_0)
11
TCP connection
SPAM blocker
18
TCP connection
gateway
13
mail queue
message transfer agent (MTA_1)
12
receiving host
message transfer agent (MTA)
14
message transfer agent (MTA)
message transfer agent (MTA)
17
mail user agent (MUA)
user mailboxes
15
16
user at a terminal

Fig. 2

CONNECTION ESTABLISHMENT
S: 220
F: 421

HELO
S: 250
E: 500, 501, 504, 421

MAIL
S: 250
F: 552, 451, 452
E: 500, 501, 421

RCPT
S: 250, 251
F: 550, 551, 552, 553, 450, 451, 452
E: 500, 501, 503, 421

DATA
I: 354 -> data -> S: 250
F: 552, 554, 451, 452
F: 451, 554
E: 500, 501, 503, 421

RSET
S: 250
E: 500, 501, 504, 421

SEND
S: 250
F: 552, 451, 452
E: 500, 501, 502, 421

SOML
S: 250
F: 552, 451, 452
E: 500, 501, 502, 421

SAML
S: 250
F: 552, 451, 452
E: 500, 501, 502, 421

VRFY
S: 250, 251
F: 550, 551, 553
E: 500, 501, 502, 504, 421

EXPN
S: 250
F: 550
E: 500, 501, 502, 504, 421

HELP
S: 211, 214
E: 500, 501, 502, 504, 421

NOOP
S: 250
E: 500, 421

QUIT
S: 221
E: 500

TURN
S: 250
F: 502
E: 500, 503

Fig. 3 (prior art)

214 Help message
[Information on how to use the receiver or the meaning of a particular non-standard command; this reply is useful only to the human user]
220 <domain> Service ready
221 <domain> Service closing transmission channel
250 Requested mail action okay, completed
251 User not local; will forward to <forward-path>

354 Start mail input; end with <CRLF>.<CRLF>

421 <domain> Service not available, closing transmission channel
[This may be a reply to any command if the service knows must shut down]
450 Requested mail action not taken: mailbox unavailable [E.g., mailbox busy]
451 Requested action aborted: local error in processing
452 Requested action not taken: insufficient system storage

500 Syntax error, command unrecognized [This may include errors such as command line too long]
501 Syntax error in parameters or arguments
502 Command not implemented
503 Bad sequence of commands
504 Command parameter not implemented
550 Requested action not taken: mailbox unavailable [E.g., mailbox not found, no access]
551 User not local; please try <forward-path>
552 Requested mail action aborted: exceeded storage allocation
553 Requested action not taken: mailbox name not allowed [E.g., mailbox syntax incorrect]
554 Transaction failed

Fig. 4 (prior art)

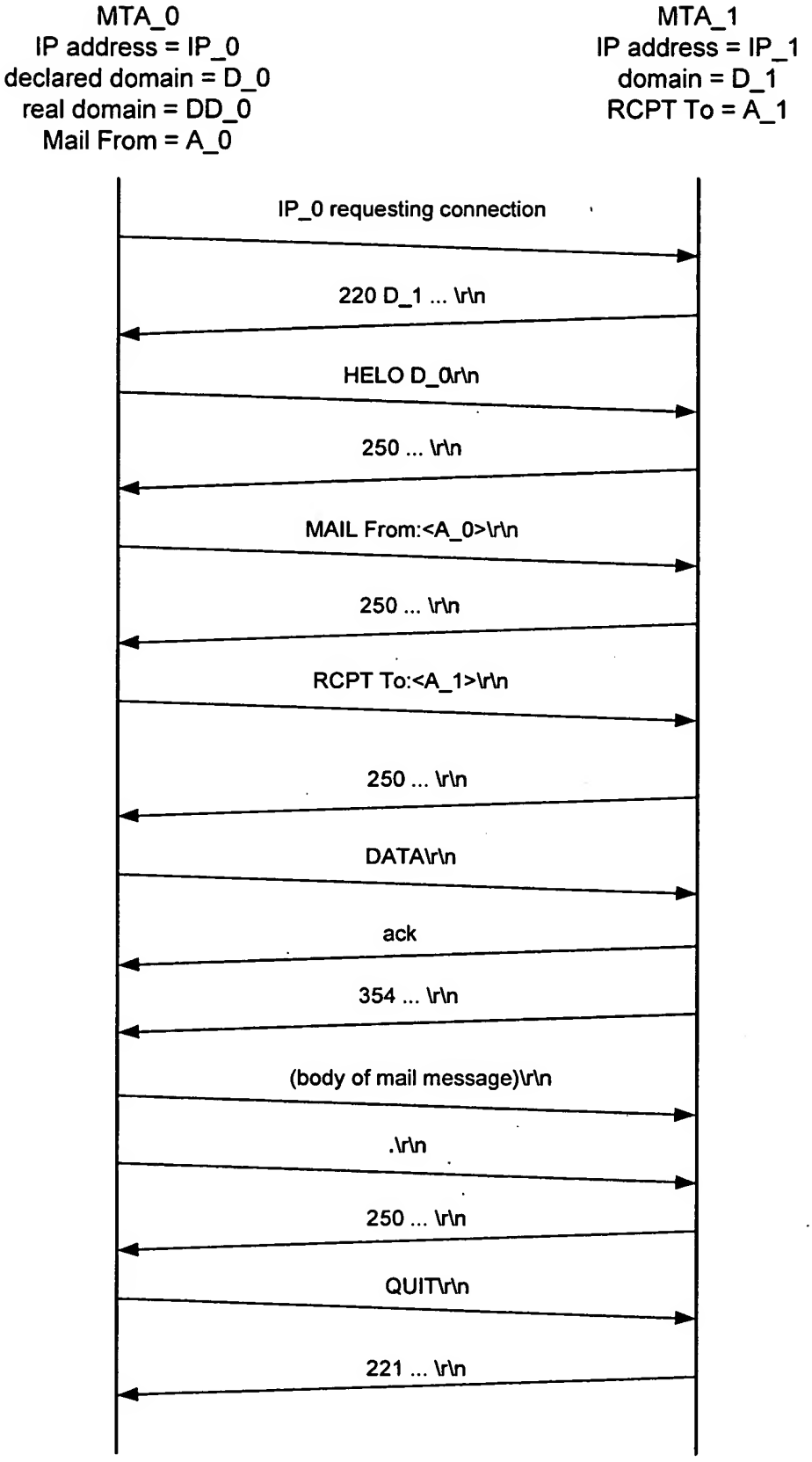

Fig. 5

(prior art)

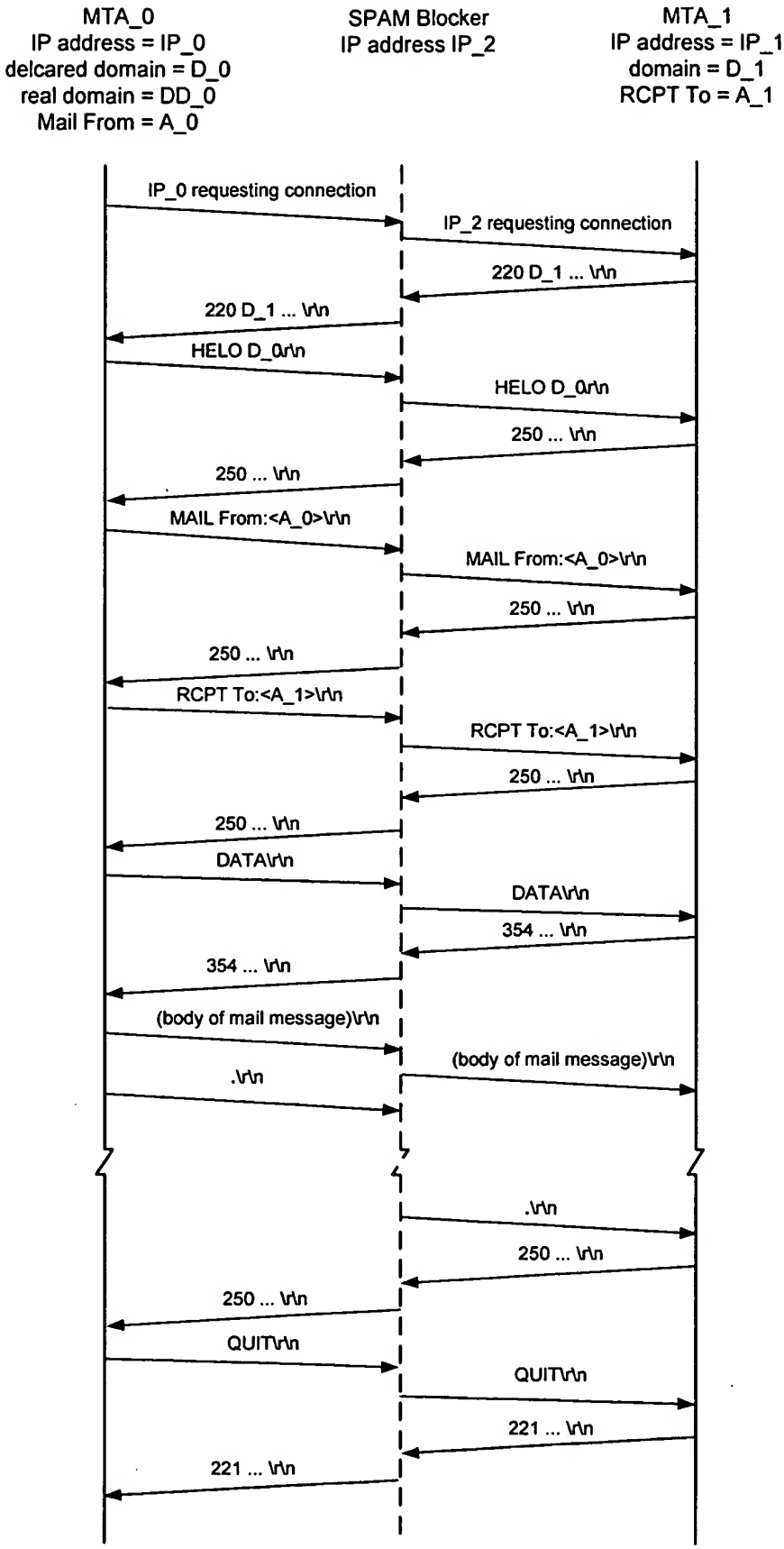
MTA_0
IP address = IP_0
delcared domain = D_0
real domain = DD_0
Mail From = A_0
SPAM Blocker
IP address IP_2
MTA_1
IP address = IP_1
domain = D_1
RCPT To = A_1
IP_0 requesting connection
IP_2 requesting connection
220 D_1 ... \r\n
220 D_1 ... \r\n
HELO D_0\r\n
HELO D_0\r\n
250 ... \r\n
250 ... \r\n
MAIL From:<A_0>\r\n
MAIL From:<A_0>\r\n
250 ... \r\n
250 ... \r\n
RCPT To:<A_1>\r\n
RCPT To:<A_1>\r\n
250 ... \r\n
250 ... \r\n
DATA\r\n
DATA\r\n
354 ... \r\n
354 ... \r\n
(body of mail message)\r\n
(body of mail message)\r\n
.\r\n
.\r\n
250 ... \r\n
250 ... \r\n
QUIT\r\n
QUIT\r\n
221 ... \r\n
221 ... \r\n

Fig. 6

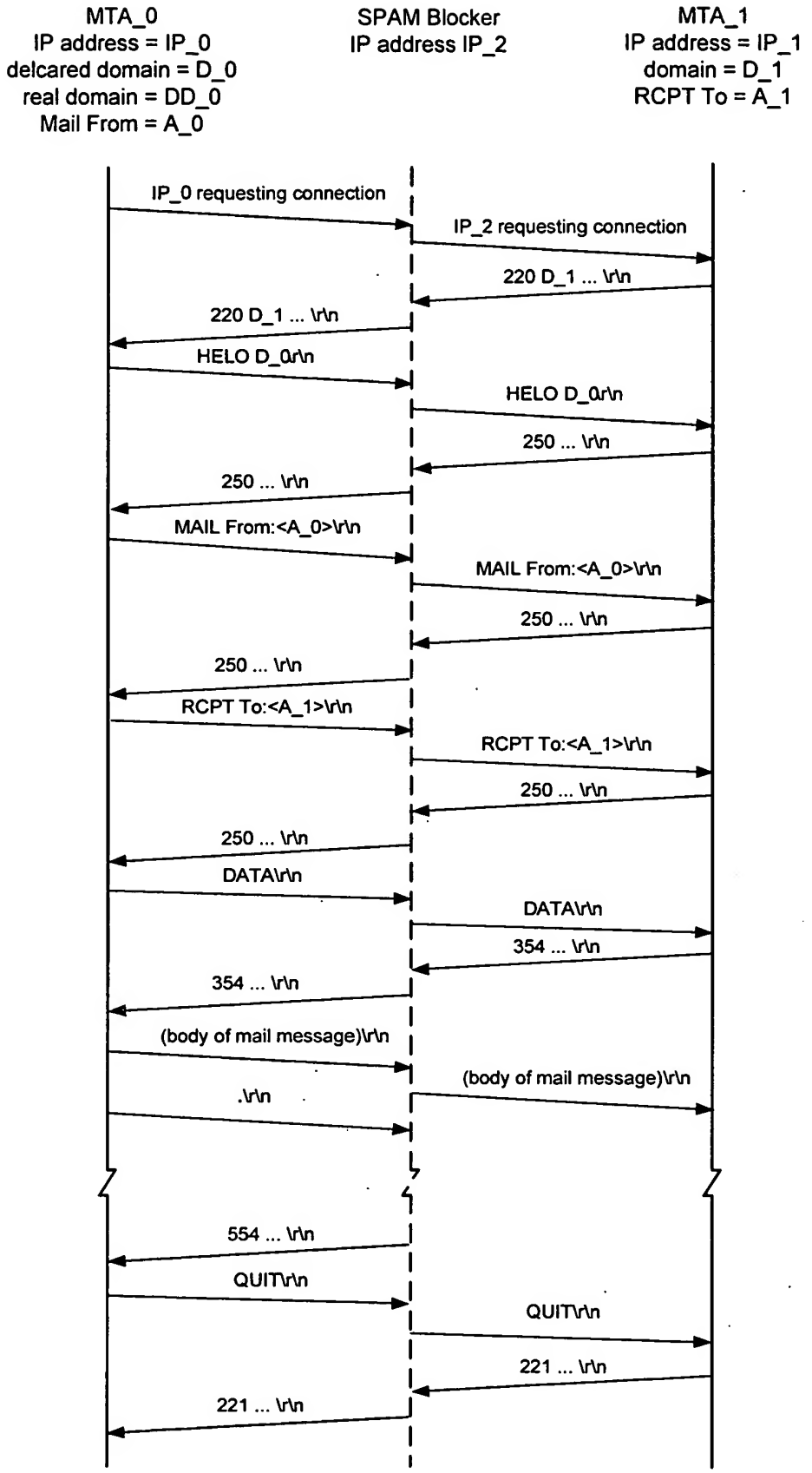
MTA_0
IP address = IP_0
delcared domain = D_0
real domain = DD_0
Mail From = A_0
SPAM Blocker
IP address IP_2
MTA_1
IP address = IP_1
domain = D_1
RCPT To = A_1
IP_0 requesting connection
IP_2 requesting connection
220 D_1 ... \r\n
220 D_1 ... \r\n
HELO D_0\r\n
HELO D_0\r\n
250 ... \r\n
250 ... \r\n
MAIL From:<A_0>\r\n
MAIL From:<A_0>\r\n
250 ... \r\n
250 ... \r\n
RCPT To:<A_1>\r\n
RCPT To:<A_1>\r\n
250 ... \r\n
250 ... \r\n
DATA\r\n
DATA\r\n
354 ... \r\n
354 ... \r\n
(body of mail message)\r\n
(body of mail message)\r\n
.\r\n
554 ... \r\n
QUIT\r\n
QUIT\r\n
221 ... \r\n
221 ... \r\n

Fig. 7

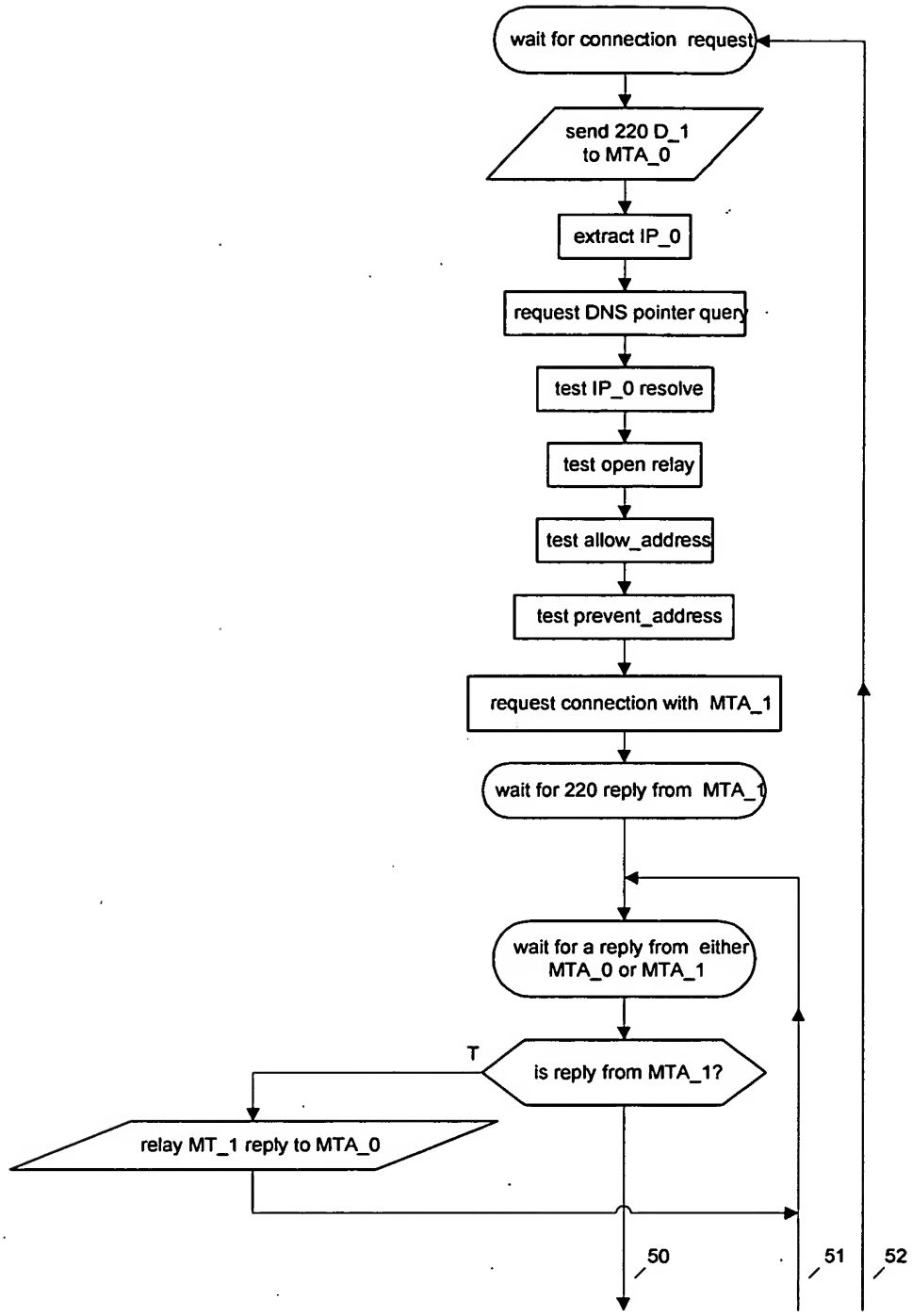
wait for connection request
send 220 D_1 to MTA_0
extract IP_0
request DNS pointer query
test IP_0 resolve
test open relay
test allow_address
test prevent_address
request connection with MTA_1
wait for 220 reply from MTA_1
wait for a reply from either MTA_0 or MTA_1
T
is reply from MTA_1?
relay MT_1 reply to MTA_0
50
51
52

Fig. 8A

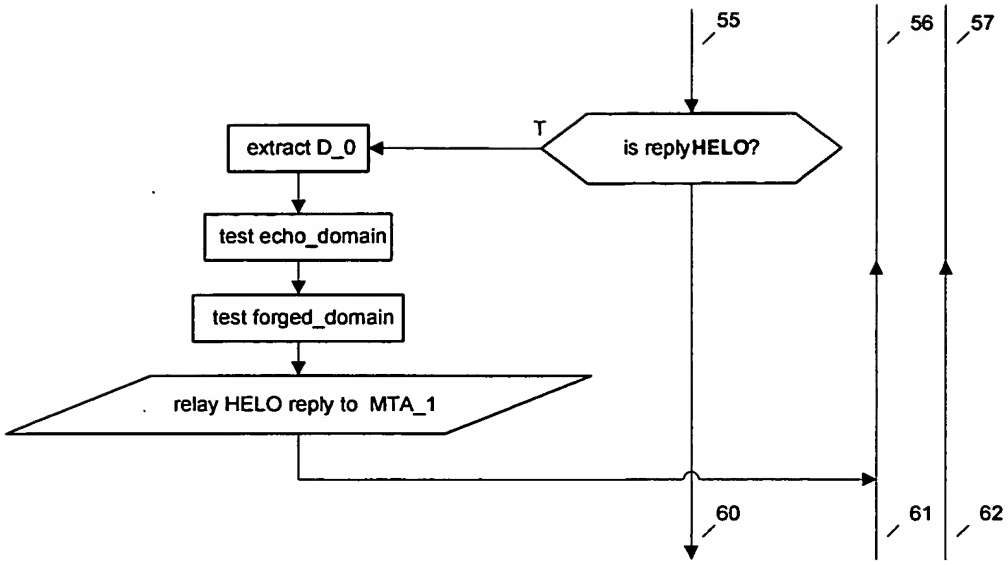
55
56
57
T
is reply HELO?
extract D_0
test echo_domain
test forged_domain
relay HELO reply to MTA_1
60
61
62

Fig. 8B

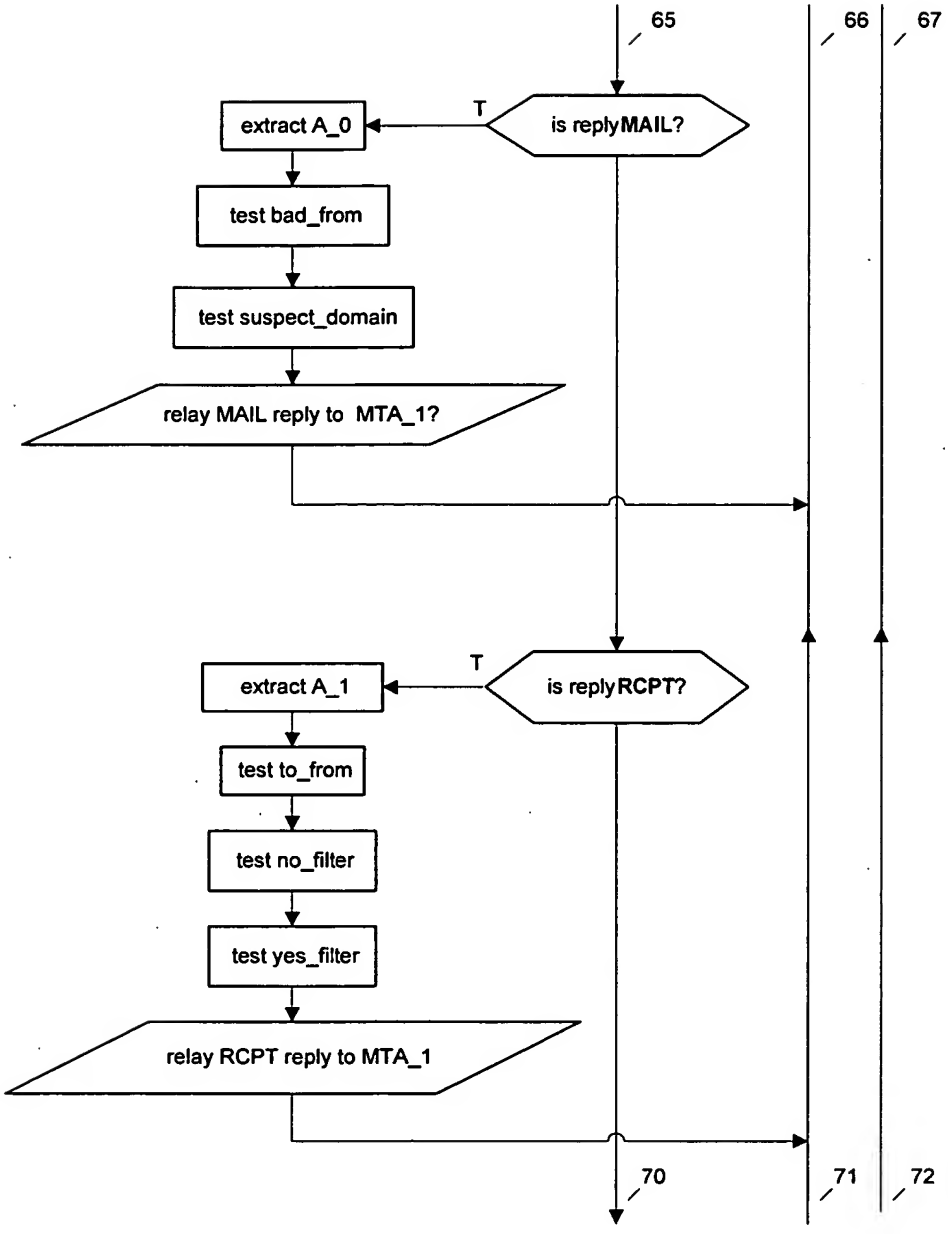
65
66
67
T
is replyMAIL?
extract A_0
test bad_from
test suspect_domain
relay MAIL reply to MTA_1?
T
is replyRCPT?
extract A_1
test to_from
test no_filter
test yes_filter
relay RCPT reply to MTA_1
70
71
72

Fig. 8C

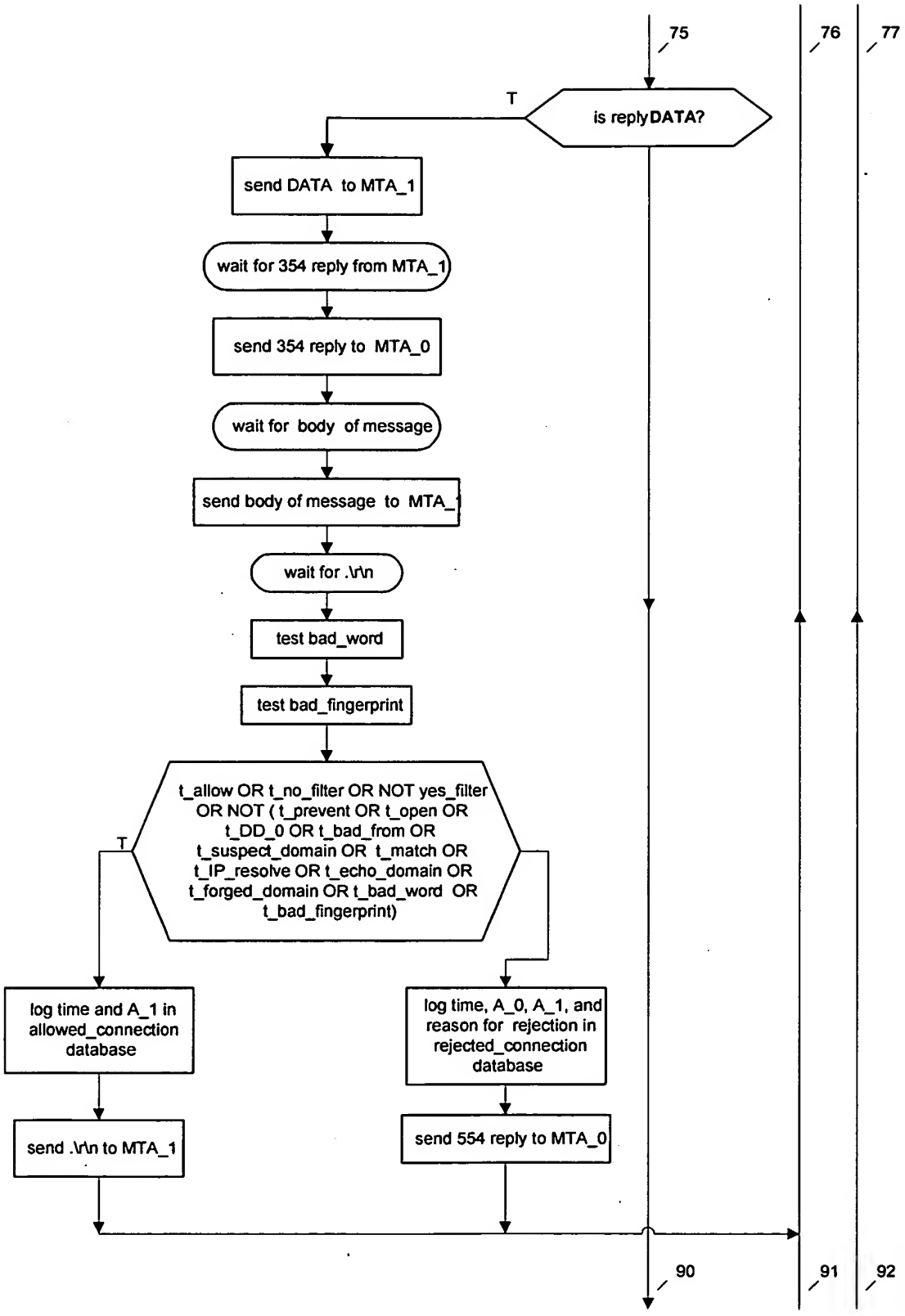
75
76
77
T
is reply DATA?
send DATA to MTA_1
wait for 354 reply from MTA_1
send 354 reply to MTA_0
wait for body of message
send body of message to MTA_1
wait for .\r\n
test bad_word
test bad_fingerprint
t_allow OR t_no_filter OR NOT yes_filter OR NOT (t_prevent OR t_open OR t_DD_0 OR t_bad_from OR t_suspect_domain OR t_match OR t_IP_resolve OR t_echo_domain OR t_forged_domain OR t_bad_word OR t_bad_fingerprint)
T
log time and A_1 in allowed_connection database
send .\r\n to MTA_1
log time, A_0, A_1, and reason for rejection in rejected_connection database
send 554 reply to MTA_0
90
91
92

Fig. 8D

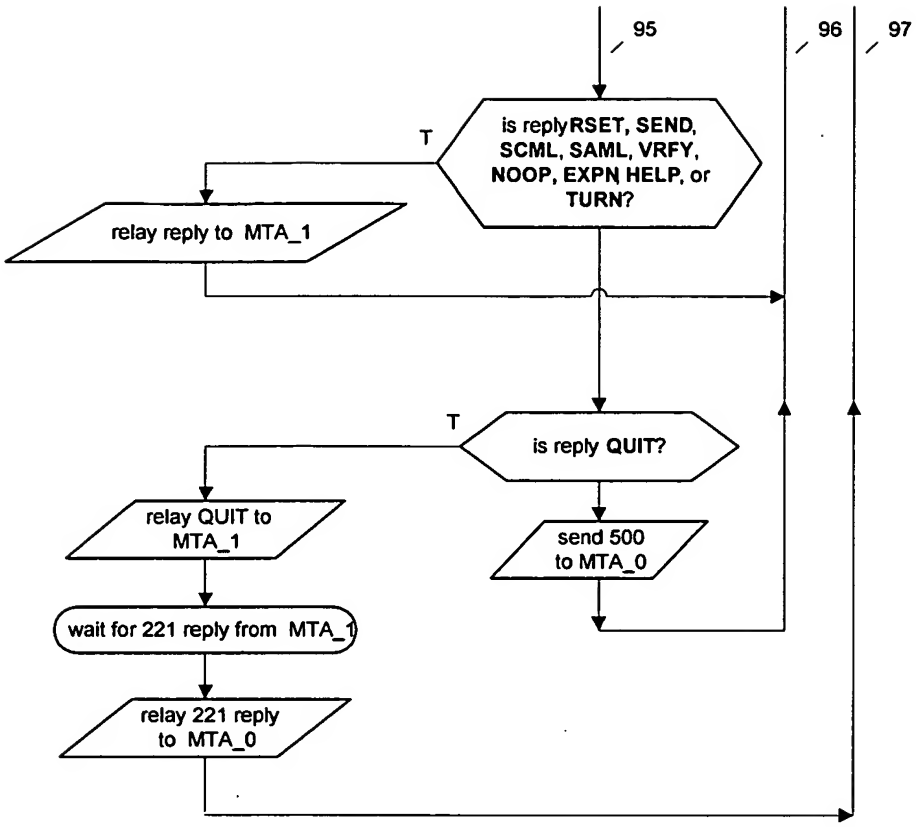
95
96
97
is reply RSET, SEND, SCML, SAML, VRFY, NOOP, EXPN, HELP, or TURN?
T
relay reply to MTA_1
is reply QUIT?
T
relay QUIT to MTA_1
send 500 to MTA_0
wait for 221 reply from MTA_1
relay 221 reply to MTA_0

Fig. 8E

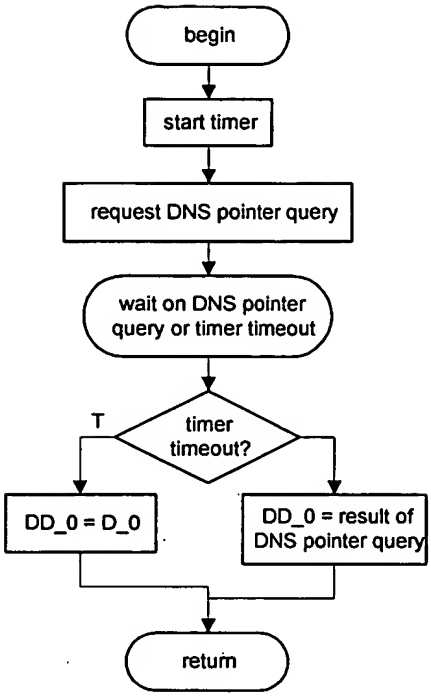
begin
start timer
request DNS pointer query
wait on DNS pointer query or timer timeout
timer timeout?
T
DD_0 = D_0
DD_0 = result of DNS pointer query
return

Fig. 9

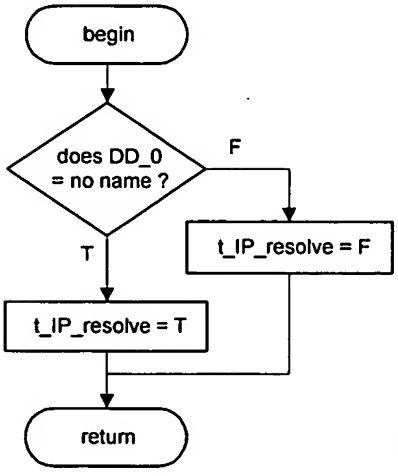
begin
does DD_0 = no name ?
F
T
t_IP_resolve = F
t_IP_resolve = T
return

Fig. 10

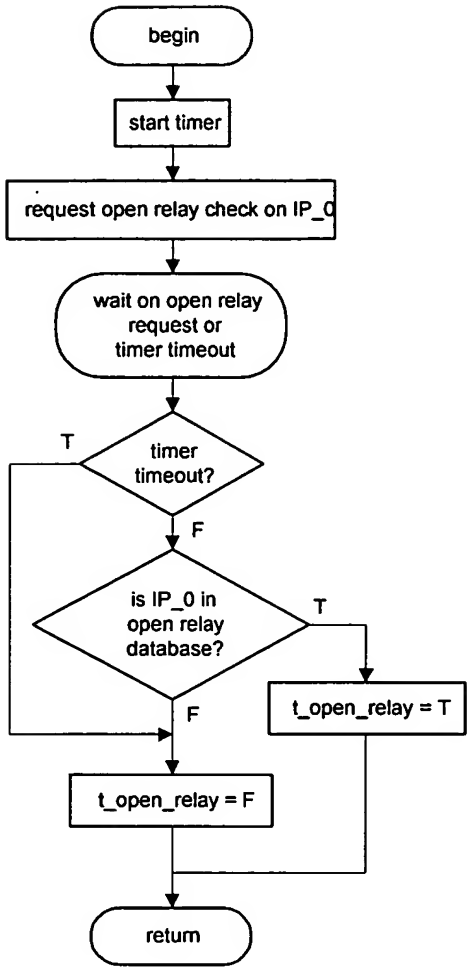
begin
start timer
request open relay check on IP_0
wait on open relay request or timer timeout
timer timeout?
T
F
is IP_0 in open relay database?
T
F
t_open_relay = T
t_open_relay = F
return

Fig. 11

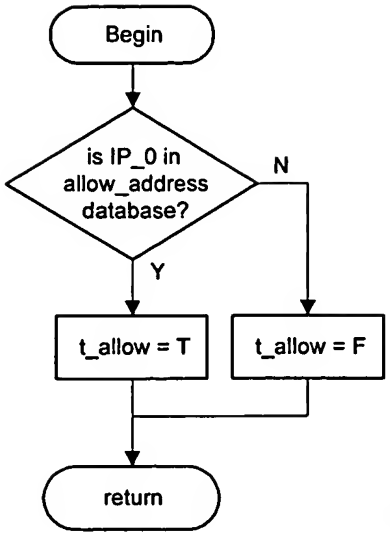

Fig. 12A

allow IP address

Fig.12B

66.75.160.12	65.54.232.7	64.4.55.7	64.4.50.7
65.54.254.145	64.4.56.135	64.4.55.135	64.4.49.199
65.54.232.71	64.4.55.71	64.4.50.71	64.4.49.135

Fig. 12C

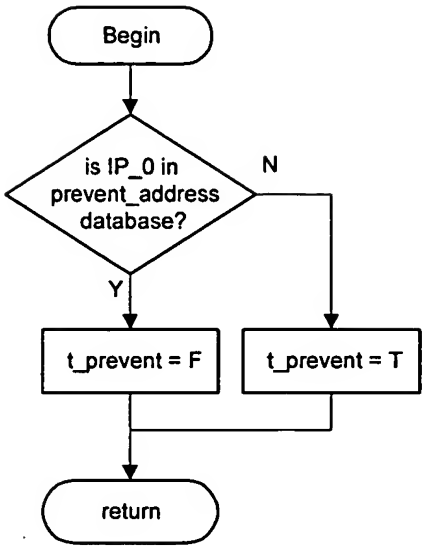

Fig. 13A

low prevent address	high prevent IP address

Fig. 13B

4.19.93.159	12.237.79.6	64.3.236.18	66.75.*.*
4.43.46.14	61.16.2.72	65.171.144.13	128.121.16.241
4.43.46.15	63.162.162.157	65.174.29.52	128.121.16.248
4.43.46.17	63.163.139.83	65.211.149.230	129.71.235.57
12.101.140.178	64.0.241.210	65.88.90.10	131.161.40.61
12.101.199.26	64.14.127.28	66.115.47.112	139.130.177.67
12.101.61.98	64.159.91.198	66.115.47.144	146.243.16.156
12.109.16.67	64.251.16.152	66.123.51.203	148.235.134.146
12.129.205.65	64.251.16.153	66.47.187.38	148.235.89.20
12.129.205.84	64.251.16.154	66.74.*.*	

Fig. 13C

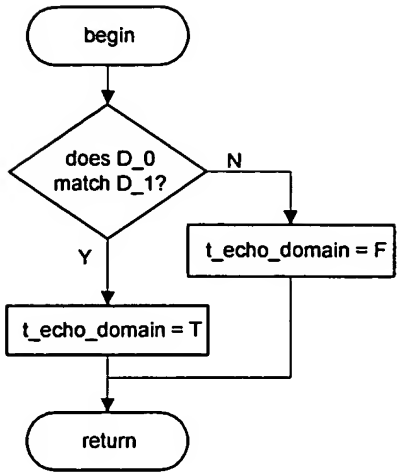
begin
does D_0 match D_1?
N
Y
t_echo_domain = F
t_echo_domain = T
return

Fig. 14

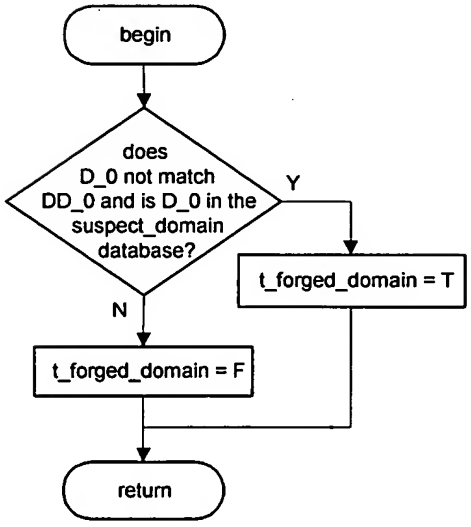
begin
does D_0 not match DD_0 and is D_0 in the suspect_domain database?
Y
N
t_forged_domain = T
t_forged_domain = F
return

Fig. 15

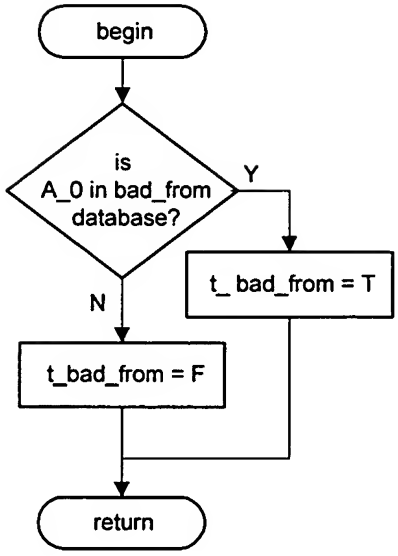

Fig. 16A

bad from address

Fig. 16B

@.cl
*@thejanusgroup.com
*@*nymphos*
*@*ramshack.net
*@freegasdaily.com
*@*emailsvc.net
*@*bbwgroup.com
*@*hostingcheck.com
*@*linksynergy.com
*@*barota.com
@.nl
*@netpaloffers.com
@.no
*@*porn*
*@*mercadobr.com
*@*medianetgroup.net
*@*myrealbox.com
*@*aweber.com
@.br
*@*agoramail.net
ipas@*
*@yourmailsource.com
fuck*.*
fuck.*
@.in

Fig. 16C

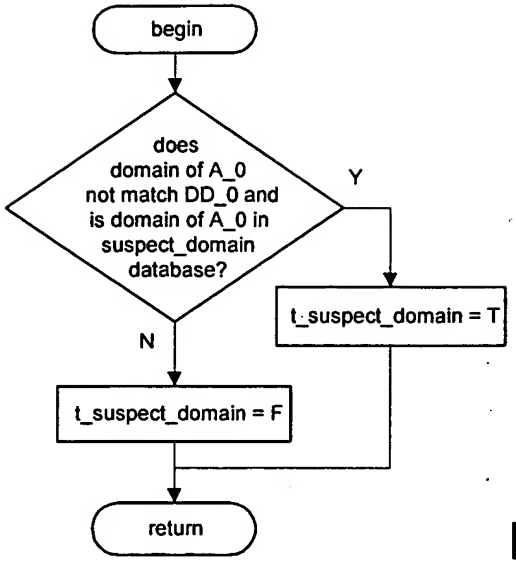

Fig. 17A

suspect domain address

Fig. 17B

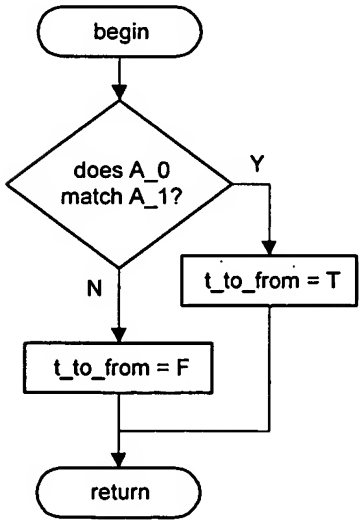

Fig. 18

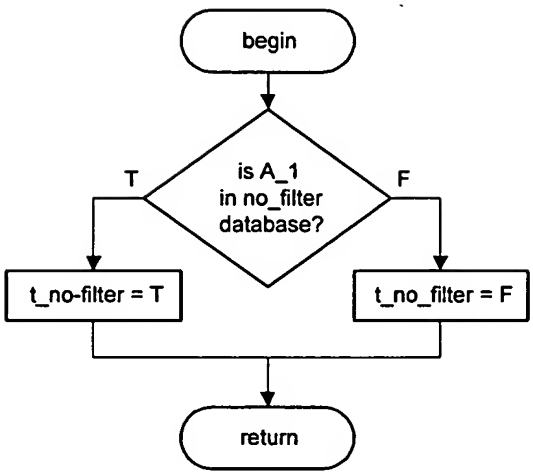

Fig. 19A

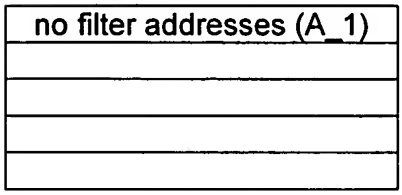

Fig. 19B

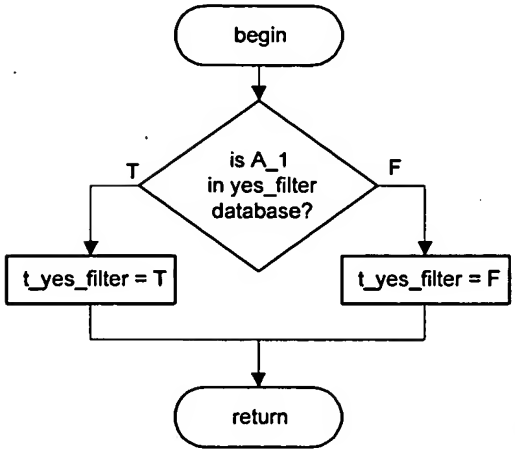

Fig. 20A

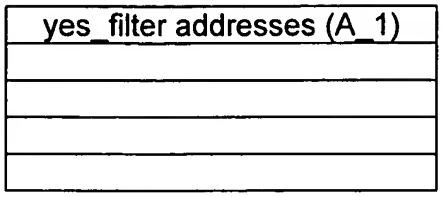

Fig. 20B

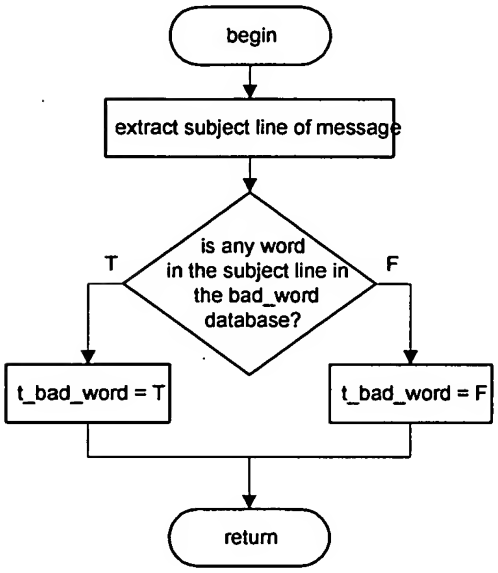

Fig. 21A

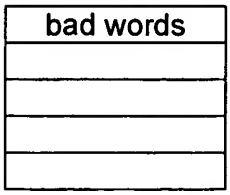

Fig. 21B

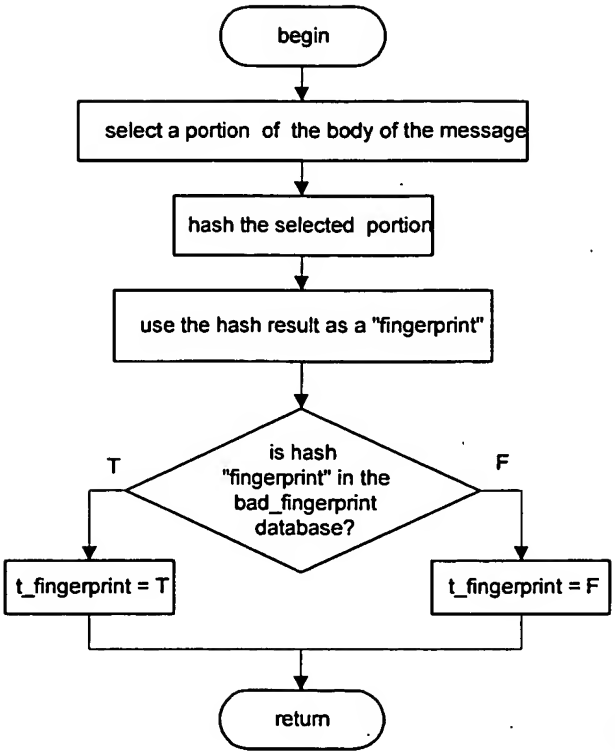

Fig. 22A

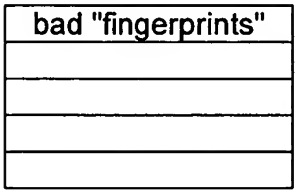

Fig. 22B

time	"To" address (A_1)

Fig. 23

time	"To" address (A_1)	"From" address (A_0)	reason for rejection

Fig. 24